Armand de Bourbon’s

Poly-Homophonic Cipher – 1649

George Lasry
The DECRYPT Project
george.lasry@gmail.com

Abstract

We deciphered two letters from 26 and 27 March 1649, from Armand de Bourbon, Prince de Conti, a leader of the Fronde. Probably addressed to the marquis Louis II de La Trémoille-Noirmoutier, they discuss recent developments in the Parliament of Paris and in French provinces. The cipher is poly-homophonic, a combination of a homophonic cipher, where each plaintext letter may be represented by several cipher symbols, and a polyphonic cipher, where a cipher symbol may represent several plaintext letters. To the best of our knowledge, this is the only documented example of such a cipher.

1 Introduction

In Lachenicht and Braun (2021, p.87), Camille Desenclos mentions a cipher, from Armand de Bourbon, Prince de Conti.[1] Two letters using this cipher have been identified in the Bibliothèque Nationale de France, Français 3584 f.113r, f113v, and f.115.[2] The second letter (f.115) is shown in Figure 1. It contains fragments of French cleartext, such as “A Paris ce 27 Mars 1649”, “j’ay cru vous debvoir”, or the signature “Armand de Bourbon”. The rest is in cipher, using lower-case letters to encipher the original text. Those letters had not been deciphered prior to this present work.

We present, in Section 2, the process of recovering the cipher key and of deciphering the letters. Section 3 provides a short historical background. The deciphered text and its translation are presented in Section 4. Some concluding remarks are given in Section 5.

2 Deciphering the letters

We first transcribed the two documents, then applied to those documents (combined) a computerized codebreaking algorithm developed by the CrypTool 2 team to solve homophonic ciphers, obtaining a tentative decryption and an initial key.[3] With additional manual work, as well as linguistic analysis of tentative decryptions, we were able to reconstruct the cipher key and complete the decipherment of the letters.

2.1 Initial computerized codebreaking

Using the computerized codebreaking algorithm, and assuming that the cipher was homophonic, we obtained the initial key shown in Figure 2. Interestingly, two homophones are assigned to each of the plaintext letters L and R. All the other plaintext letters have only one homophone, which is not typical of contemporary homophonic ciphers, where the vowels and the most frequent letters were usually assigned more than one cipher symbol. With this initial key, we obtained an initial decipherment of the second letter, shown in Figure 3.[4]

[1] Armand de Bourbon, Prince of Conti (1629 – 1666). French nobleman, brother of the Grand Condé. His sister married Henri II d'Orléans-Longueville. He was at time a patron of Molière, the famous French playwright and actor, turning later against him on religious grounds.

[2] Additional letters encoded with this cipher may exist.

[3] The algorithm is described in Kopal (2021).

[4] Due to lack of space, we do not show the decipherment of the first letter.

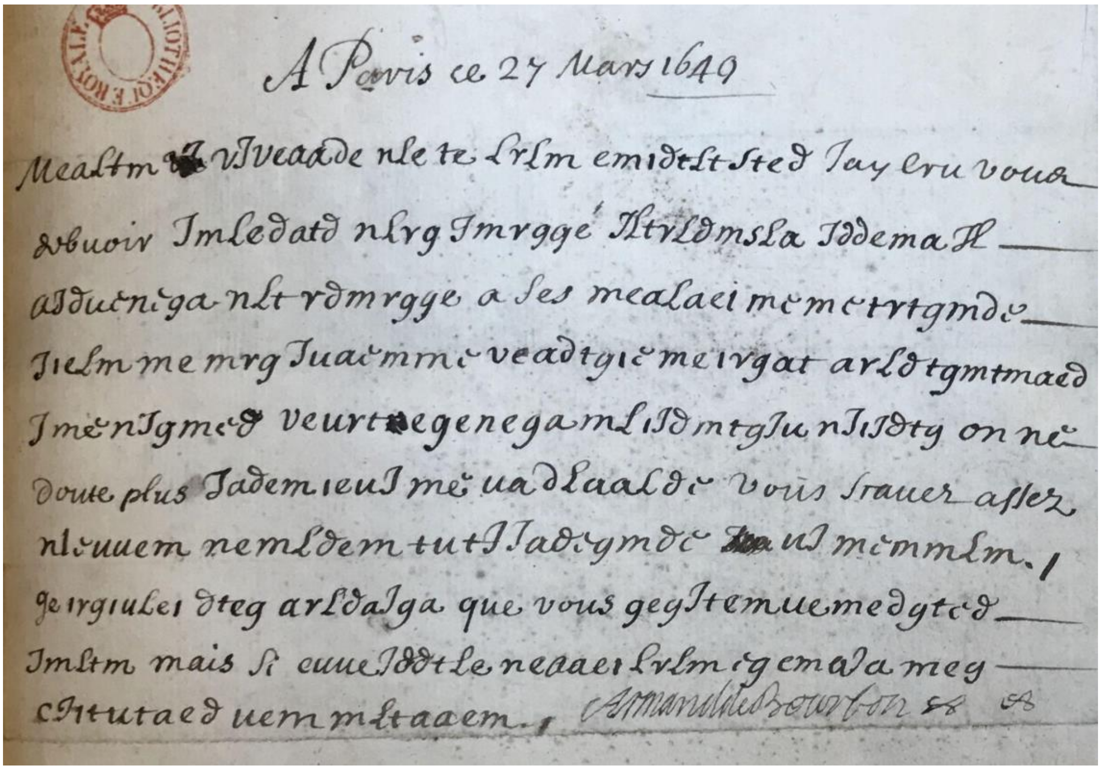

A Paris ce 27 Mars 1649
J'ay cru vous
debvoir
a ses
on ne
doute plus
vous scaver assez
que vous
mais si
Armand de Bourbon

Figure 1 - Second letter - 27 March 1649 (Source: gallica.bnf.fr / BnF fr. 3584 f.115)

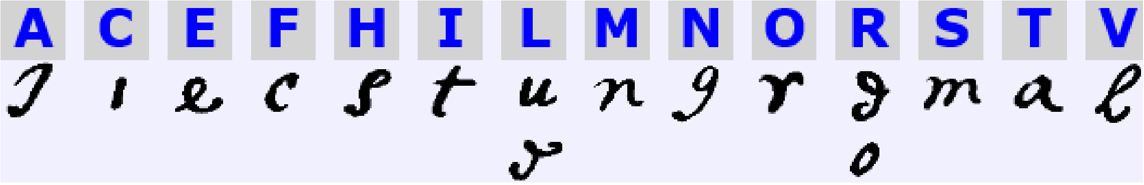
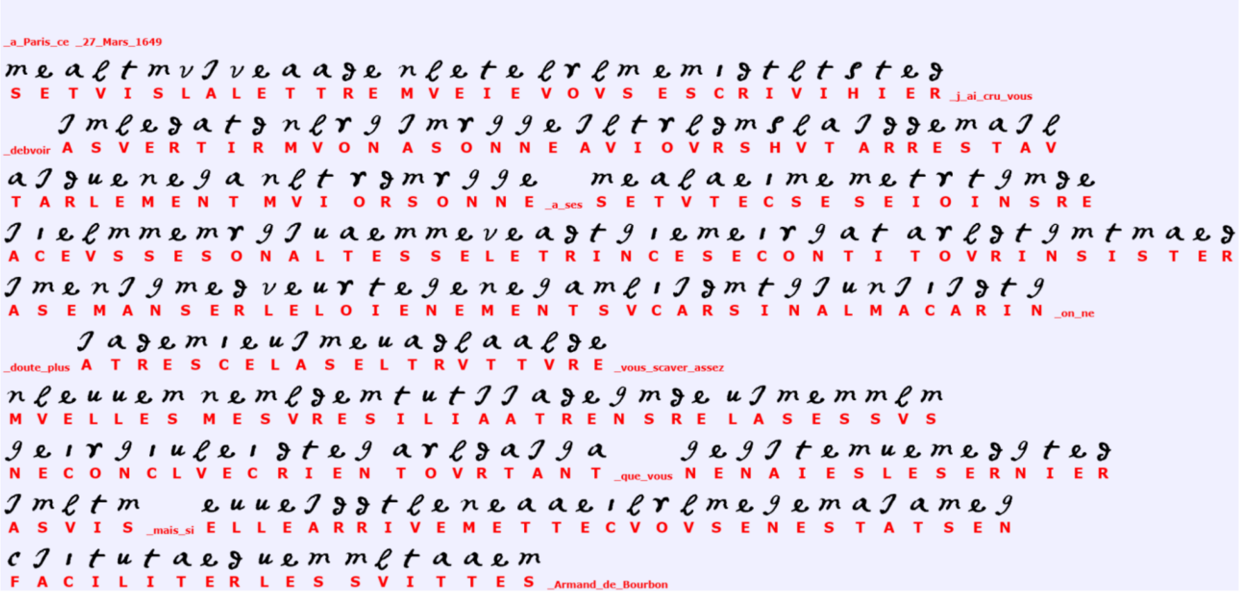

A
C
E
F
H
I
L
M
N
O
R
S
T
V

Figure 2 – Initial key



_a_Paris_ce _27_Mars_1649

SETVISLALETTREMVEIEVOVSESCRIVIHIER _j_ai_cru_vous

_debvoir ASVERTIRMVONASONNEAVIOVRSHVTARRESTAV

TARLEMENTMVIORSONNE _a_ses SETVTECSESEIOINSRE

ACEVSSESONALTESSELETRINCESECONTITOVRINSISTER

ASEMANSERLELOIENEMENTSVCARSINALMACARIN _on_ne

_doute_plus ATRESCELASELTRVTTVRE _vous_scaver_assez

MVELLESMESVRESILIAATRENSRELASESSVS

NECONCLVECRIENTOVRTANT _que_vous NENAIESLESERNIER

ASVIS _mais_si ELLEARRIVEMETTECVOVSENESTATSEN

FACILITERLESSVITTES _Armand_de_Bourbon

Figure 3 – Initial decryption of the second letter

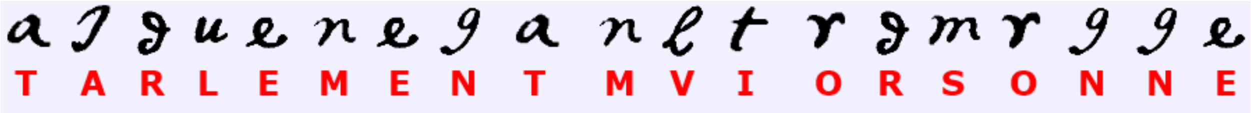


Figure 4 – Fragment of deciphered text with errors – Example 1

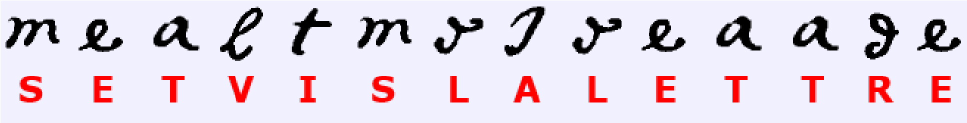


Figure 5 – Fragment of deciphered text with errors – Example 2

Most of the deciphered text consists of plausible fragments of French, or full French words or expressions. For example, the last line FACILITERLESSVUITES reads as "faciliter les suites" ("to facilitate the follow-up"). But many other fragments seem to contain one or more errors, which cannot be easily resolved. For example, the beginning of the fragment shown in Figure 4, "TARLEMENT" seems to be "PARLEMENT". But if we simply try to assign the homophone 'a' to the letter P instead of the current assignment to T, we obtain "PARLEMENP" which is also wrong.

Similarly, the fragment "SETUISLALETTRE" shown in Figure 5 seems to read "depuis la lettre" ("since the letter"). But if we try to assign the homophone "m" to the letter D instead of to S, and we also try to assign 't' to P instead of to T, we obtain "DEPUIDLALEPPRE" ("depuid la leppre"), which is also wrong.

So obviously, under the assumption that this is a purely homophonic cipher, there is no way to "fix" the key so that all those errors (we spotted over 150 such discrepancies) may be corrected.

2.2 Manual decipherment

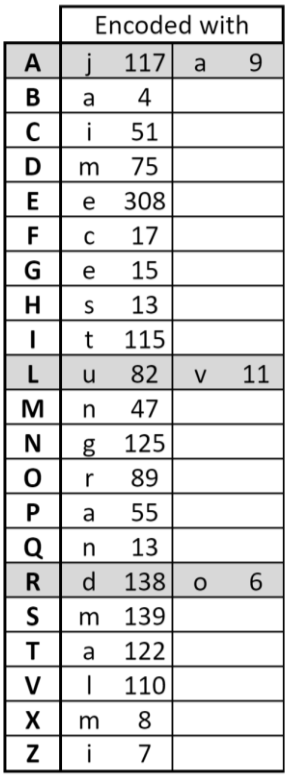
To determine the precise structure of the cipher, the next step was to recover the original plaintext, starting from the parts that looked fully or partially plausible. After extensive trial-and-error, we were able to recover most of the original text. We then counted the number of times each plaintext letter is represented by a certain cipher symbol, as shown in Figure 6. For example, the cipher symbol 'a' represents the letter T 122 times, the letter P 55 times, the letter A nine times, and the letter B four times.

	Decodes as							
a	T	122	P	55	A	9	B	4
c	F	17						
d	R	139						
e	E	308	G	15				
g	N	125						
i	C	51	Z	7				
j	A	117						
l	V	110						
m	S	138	D	75	X	8		
n	M	47	Q	13				
o	R	6						
r	O	89						
s	H	13						
t	I	115						
u	L	82						
v	L	11						

Figure 6 – Evidence for polyphony

From the segment in Figure 4, we had already concluded that 'a' could either represent T or P. With the complete data in Figure 6, we can see that 'a' may also represent A or B. Similarly, from the segment in Figure 5, we had already concluded that 'm' could represent either S or D, and in Figure 6 we see that it may also represent X. In summary, for five symbols ('a', 'e', 'i', 'm', and 'n'), there are two to four possible interpretations, which is consistent with a polyphonic cipher.

We also produced the reversed analysis, showing the breakdown of which cipher symbols are used to encode a certain plaintext letter, as shown in Figure 7.



	Encoded with			
A	j	117	a	9
B	a	4		
C	i	51		
D	m	75		
E	e	308		
F	c	17		
G	e	15		
H	s	13		
I	t	115		
L	u	82	v	11
M	n	47		
N	g	125		
O	r	89		
P	a	55		
Q	n	13		
R	d	138	o	6
S	m	139		
T	a	122		
V	l	110		
X	m	8		
Z	i	7		

Figure 7 – Evidence for homophony

Figure 7 shows that each of the three plaintext letters, A, L, and R, has two homophones.

While the evidence for polyphony is somehow stronger than the evidence for homophony,[5] there is enough evidence to establish that we have here a new type of cipher, a poly-homophonic cipher, which combines the two types.

We show in Figure 8 the final decipherment of the second letter. There are still a few errors, such as “AVIOURDVT” which should be “AVIOURDVI” (“aujourd’hui”, today) on the second line, but those kinds of sporadic errors are expected in any enciphered document.

The complete decipherment, after correcting the remaining errors, and formatting the text, is shown in Section 4.

2.3 The cipher key

We show the final key in Figure 9. As described in Lachenicht and Braun (2021), most French ciphers in the 16th and 17th centuries were homophonic. Polyphonic ciphers were less prevalent, and those documented were primarily used by papal nuncios in the 16th century (Meister 1906). An example of a polyphonic French cipher, used by the Duc de Mayenne, is given in Tomokiyo (2019). In addition, most contemporary ciphers also had a nomenclature, with additional symbols to encode entire words, names, and parts of words.

In contrast with most contemporary ciphers, the cipher used by Armand de Bourbon has no nomenclature, and it combines polyphony with homophony. The author is not aware of any other example of such a poly-homophonic cipher. While more secure, such a cipher would also have been difficult to employ when enciphering a text, and even more difficult when deciphering a ciphertext, even if the key was known to both parties.

One of the reviewers of this paper has noticed that the second column of Figure 7 may be read as a keyword (or key expression), as follows: *jaimecestungrandmal* (*J’aime c’est un grand mal*).[6] This happens to be the title of an *air de cour* composed by Antoine Boesset in 1642.[7] The year is too close to the time the letters were sent and the key expression too long to be a coincidence. So, it is very likely that the two correspondents relied on this shared expression to exchange or remember the key.

[5] One may argue that this cipher is only weakly homophonic. On the one hand, there are only three letters of the alphabet represented by more than one cipher symbol, and among them, the use of the homophone ‘a’ to encipher the letter A might be due to confusion – the same letter being wrongly enciphered with itself. On the other hand, this may also indicate a “lazy” use of the homophones, the person enciphering the letter almost always using only one of the two homophones assigned to each letter.

[6] Loosely translated as *I love this hurts badly*.

[7] According to Wikipedia, the *air de cour* was a popular type of secular vocal music in France in the late Renaissance and early Baroque period, from about 1570 until around 1650.

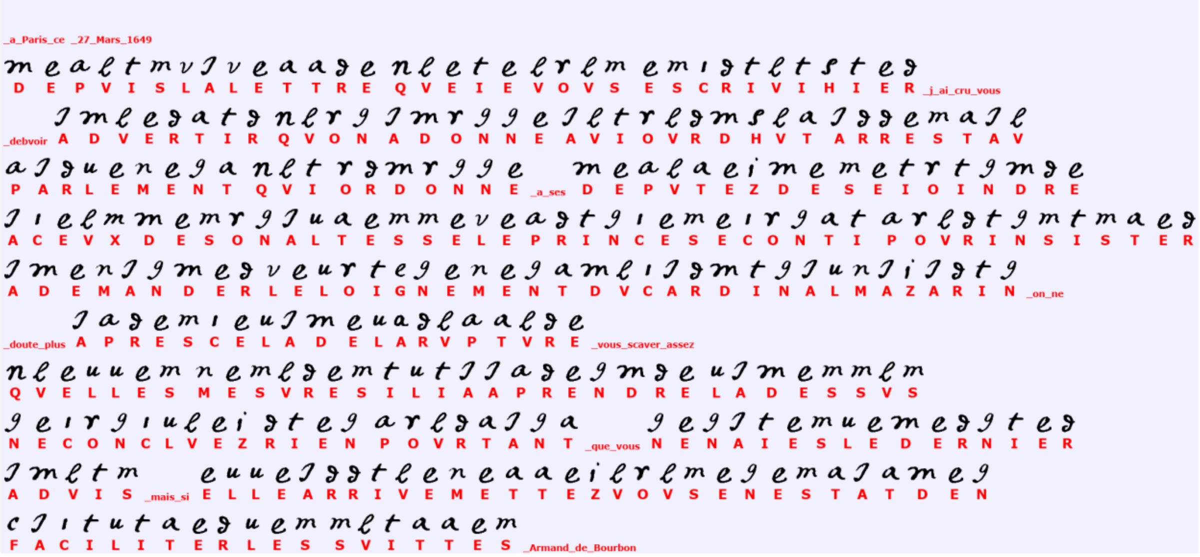

_a_Paris_ce _27_Mars_1649
D E P V I S L A L E T T R E Q V E I E V O V S E S C R I V I H I E R _j_ai_cru_vous
_debvoir A D V E R T I R Q V O N A D O N N E A V I O V R D H V T A R R E S T A V
P A R L E M E N T Q V I O R D O N N E _a_ses D E P V T E Z D E S E I O I N D R E
A C E V X D E S O N A L T E S S E L E P R I N C E S E C O N T I P O V R I N S I S T E R
A D E M A N D E R L E L O I G N E M E N T D V C A R D I N A L M A Z A R I N _on_ne
_doute_plus A P R E S C E L A D E L A R V P T V R E _vous_scaver_assez
Q V E L L E S M E S V R E S I L I A A P R E N D R E L A D E S S V S
N E C O N C L V E Z R I E N P O V R T A N T _que_vous N E N A I E S L E D E R N I E R
A D V I S _mais_si E L L E A R R I V E M E T T E Z V O V S E N E S T A T D E N
F A C I L I T E R L E S S V I T T E S _Armand_de_Bourbon

Figure 8 – Final decryption of the second letter

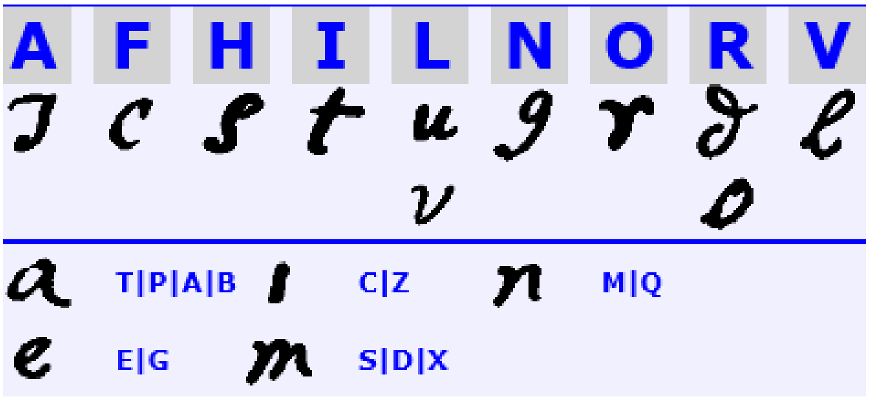


Figure 9 – Final key

3 Historical background

Before presenting the full deciphered text, we provide here a short historical background about the Fronde, and the Parliamentary Fronde (the First Fronde) in particular.[8]

3.1 The Fronde

The Fronde was a series of civil wars and insurrections in France between 1648 and 1653, occurring during the Franco-Spanish War, which had begun in 1635, and right after the Thirty-Year War, which ended in 1648. Minor King Louis XIV (1638-1715), his regent mother Anne of Austria,[9] and Cardinal Mazarin[10] confronted the combined opposition of the princes, the nobility, and the Parliaments, but eventually managed to subdue them all. The dispute started when the government of France issued fiscal edicts to increase taxation. The Parliament of Paris resisted and sought to check the King's powers. The Fronde was divided into three phases, the Parliamentary Fronde (1648-49), the Fronde of the Princes (1650-1651), and the Fronde of Condé (1651-1652). Cardinal Mazarin blundered into the crisis but came out well ahead at the end.

3.2 The First Fronde – the Parliamentary Fronde

The First Fronde – the Parliamentary Fronde, started in May 1648 when a tax levied on judicial officers of the Parliament of Paris provoked not

[8] The information in this background section was mostly taken from Wikipedia.

[9] Anne of Austria (1601 – 1666) was an infanta of Spain who became Queen of France as the wife of King Louis XIII from their marriage in 1615. When Louis XIII died in 1643, Anne became regent to her son Louis XIV, during his minority, until 1651. During her regency, Cardinal Mazarin served as France's chief minister.

[10] Cardinal Jules Mazarin (1602 – 1661), born Giulio Raimondo Mazzarino or Mazarini, was an Italian cardinal, diplomat and politician who served as the chief minister to the Kings of France Louis XIII and Louis XIV from 1642 to his death.

merely a refusal to pay but also a condemnation of earlier financial edicts.[11] In August 1648, Mazarin suddenly arrested the leaders of the Parliament, whereupon Paris broke into insurrection and barricaded the streets. The noble faction demanded the calling of an assembly of the Estates General. The royal faction, having no army at its immediate disposal, had to release the prisoners and to promise reforms. However, France's signing of the Peace of Westphalia allowed the French army to return from the frontiers,[12] and by January 1649, Mazarin's ally the prince de Condé had put Paris under siege.[13] The Parliament's legalist faction led by the first president Mathieu Molé and the president Henri de Mesmes pushed for negotiations. The two warring parties signed the Peace of Rueil (11 March 1649) after little blood had been shed, followed by the Peace of Saint-Germain (1 April 1649). The Parisians, under the military leadership of Armand de Bourbon, Condé's brother, having refused an offer of help from Spain, but with no prospect of military success without such external aid, eventually submitted to the government while receiving some concessions.

The two letters we deciphered were written after the Peace of Reuil, and a few days before the signature of the Peace of Saint-Germain.

4 The deciphered letters

The parts in cipher are in *italics*.

4.1 First letter

A Paris ce 26 mars 1649

Affin que Monsieur *Le Monsieur de Noirmo[u]stier*[14] *sache l'estat* des choses *positivement* comme *elles se passent à St Germain,*[15] il sera *averti* que *l'on insiste* fort dans *la conférence sur les intérêts* du *parlement de Normandie* avec lesquels le *parlement de Paris [est?] tellement joint. Que* hier *le premier président* et *le président de Mesmes* déclarèrent que si *le parlement de Normandie* n'estoit *content l'on romproit.* Les intérêts *du dit parlement sont grants* ce qui faict *croire la rupture. Que l'on insistera* fort *encore sur l'exclusion du Cardinal les députez* de Messieurs *les généraux* en ayant *eu ordre exprès*. Que l'on *demande encor positivement* et sans *qu'on en puisse relascher* que *Monsieur de Longueville*[16] *traittera* avec *Monsieur de Tenerande(?).* Que sur ces *articles on attend la rupture de laquelle on parleroit p[lu]s positivement si son Altesse* n'agessoit pas avec quelque *dépendance. Que véritablement le parlement a bien accordée la t[r]êve* mais *avec ordre positif de ne continuer* pas la *conférence après quatre jours espiréz* qui est le *temps que doit durrer la prolongation* et que *les députez s'en reviendront* dans lequel *temps les choses pouvant* pas vraisemblablement *s'ajuster, cela donne pour lieu* et croire que *la conférence se rompra.* Que l'on a esté *fort surpris de la retraite de* Monsieur *l'archiduc*[17] *du Pont-a-Vert* et l'abandonnement *des passages de la rivière*, Monsieur *le maréchal du Plessis*[18] *n'ayant que de médiocres forces et Erlac*[19] *s'avançant avec si peu de monde.* Que *cette retraite a fort mal réussi* et faict un fort *grand tort aux affaires* mais que n'y *ayant nul danger de reprendre un passage sur la rivière* cela redonneroit *chaleur aux affa[i]res et remettroit*

[11] In January 1648, Mazarin had issued those fiscal edicts, but the Parliament of Paris decided to ignore them. To convince this parliament to withdraw its opposition, Mazarin exempted it from paying for the renewal of the "Paulette". In an exceptional display of solidarity, the sovereign courts, which included the various parliaments, decided on 13 May 1649 to convene in the Palace of Justice, where the Parliament of Paris resided, starting the Parliamentary Fronde.

[12] Treaty of Münster, 24 October 1648.

[13] Louis de Bourbon, Prince de Condé (1621 – 1686), known as le Grand Condé for his military exploits, was a French general and a member of the Condé branch of the House of Bourbon, and the brother of Armand de Bourbon. Having fought on the side of the French court during the First Fronde, we rebelled against Louis XIV as the leader of the last Fronde in 1651, leading to his exile from France until 1659 when he was rehabilitated.

[14] Louis II de La Trémoille, marquis, later Duc de Noirmoutier (1612-1666), often simply called « Noirmoutier », was a nobleman and general who joined Armand de Bourbon and Longueville on the Parliament side during the First Fronde.

[15] In January 1649, the Queen Mother and King Louis XIV had fled from Paris to St. Germain, ordering that Paris be put under siege.

[16] Henri II d'Orléans, Duc de Longueville or Henri de Valois-Longueville (1595 – 1663), a prince of France of royal descent, was a major figure during the Fronde, and served as governor of Picardy, then of Normandy. He married Armand de Bourbon's sister.

[17] Archduke Leopold Wilhelm of Austria (1614 – 1662), younger brother of Emperor Ferdinand III, was an Austrian soldier, administrator, and patron of the arts. He served as Governor of the Spanish Netherlands and offered his help to the First Fronde leaders in Paris. Despite being nominated as Holy Roman Emperor after Ferdinand's death in 1657, he stood aside in favor of his nephew Leopold I.

[18] César, Duc de Choiseul, Comte du Plessis-Praslin (1602 – 1675) was a Marshal of France and French diplomat, loyal to the French court.

[19] Jean Louis d'Erlach (1595–1650) was a Swiss general and politician, who supported the French court during the First Fronde.

tout en *bon estat* ce que l'on attend *absolument* de son *altesse impér[iale]*. Que *dimanche ou lundi* on ne manquera *de vous donner advis de la dernière résolution des choses* qu'on espère telle qu'on la peut désirer y ayant *peu de lumière à l'accomodement* mais qu'au cas *qu'il se fist ce ne sera point sans faire tous les effors pour tirer* les assurances *de la p[a]ix générale.* Les *provinces sont en cet estat*: Monsieur *de Longueville a dix(six?)*[20] *mil hommes.* Que *Thoulouse* a donné *l'arrest*. Que *Bordeaux va le donner.* Que la *Provence* est en *armes avec le Poitou le Périgueux de Q[u]ercy de Limosin et* quantité *de lieus e[n] B[r]etaigne et le peuple se pris* mieux intentionné que jamais.

Paris, 26 March 1649

For Monsieur, Monsieur de Noirmoustier to positively know the state of affairs as they took place in St Germain, he should be informed that we are strongly insisting in the conference on the interests of the Parliament of Normandy, which the Parliament of Paris is joining. That yesterday, the First President and de Mesmes the President have declared that unless the Parliament of Normandy is satisfied, there will be a rupture. As the interests of the said Parliament have been granted, this rupture is expected. That we will strongly insist on the exclusion of the Cardinal, the deputies of Messieurs, the generals having been given an explicit order. That we are still positively demanding, without being able to give up, that Monsieur de Longueville deal with Monsieur de Tenerande(?). That because of those articles, a rupture is expected, which is seen more positively, unless his Highness acts with some dependence. That the Parliament has indeed accorded a truce, but with a positive order not to continue the conference for more than four additional days (which is the time of the prolongation), and the deputies will return to it, and as things are not likely to be settled by then, it is expected that the conference will adjourn. That there has been a great surprise about Monsieur the Archduke's retreat in Pont-a-Vert, and the abandonment of the crossings of the river, Monsieur the Marechal de Plessis having only some mediocre forces at his disposition, and Erlach advancing with so few men. That this retreat has badly failed, and has strongly harmed the affairs, but as there is no danger of attempting to cross the river, this would enable the affairs to be brought back to a good state, which is expected from his Imperial Highness. That Sunday or Monday, we will not fail to notify you of the latest resolution on the matters, hoping to have a better understanding about the accommodation, but in case this happens, this will not be without making every effort to obtain the assurances of the general peace. The provinces are in the following situation: Monsieur de Longueville has ten (or six?) thousand men. That Thoulouse has given the ruling. That Bordeaux is about to give it. That the Provence has taken arms with the Poitou, the Périgueux de Quercy, the Limosin, and many places in Brittany, and the people is better intentioned than ever.

4.2 Second letter

A Paris, le 27 mars 1649

Depuis la lettre que je vous escrivi hier j'ay creu vous debvoir *advertir qu'on a donné aujourd'hui arrest au parlement qui ordonne* à ses *députez de se joindre à ceux de son Altesse le Prince de Conti à demander l'éloignement du cardinal Mazarin.* On ne doute plus *après cela de la rupture.* Vous scavez assez *quelles mesures il y a à prendre là-dessus. Ne concluez rien pourtant* que vous *n'ayes le dernier advis* mais si *elle arrive mettez-vous en estat d'en faciliter les suittes.*
Armand de Bourbon

Paris, 27 March 1649

Since the letter I wrote to you yesterday, I ought to notify you that today, a ruling has been given in Parliament, which orders its deputies to join her Highness the Prince de Conti in demanding that Cardinal Mazarin be removed. There is no doubt that this will result in the rupture. You know well enough which measures should be taken about this. Nevertheless, do not conclude anything before you get the latest notice, but if this happens, be ready to facilitate what follows.

Armand de Bourbon

[20] Ambiguous, because the symbol for S is the same as the symbol for D. An example of the challenge of deciphering a polyphonic cipher, even when the key is known.

5 Conclusion

This cipher illustrates an interesting combination of two schemes of substitution ciphers, and there are no other known examples of such a poly-homophonic cipher. Also, while the letters of Armand de Bourbon are of special interest for research on the development of ciphers, their contents may also be of interest to historians.

Acknowledgments

The author would like to thank Camille Desenclos from the University of Picardie – Jules Verne for bringing this interesting cipher to light, providing copies of the documents, assisting in the interpretation of the text, and reviewing an early draft of this paper.

The author would also like to thank the anonymous reviewer for the astounding discovery of the key expression in the homophonic key table.

Funding

This work has been supported by the Swedish Research Council, grant 2018-06074, DECRYPT – Decryption of Historical Manuscripts.

References

Alois Meister. 1906. *Die Geheimschrift im Dienste der Päpstlichen Kurie von Ihren Anfängen bis zum Ende des XVI. Jahrhunderts*, vol. 11. Paderborn: F. Schoningh.

Susanne Lachenicht and Guido Braun (ed.). 2021. *Spies, Espionage and Secret Diplomacy in the Early Modern Period*. Kohlhammer Verlag.

Nils Kopal. 2019. “Cryptanalysis of homophonic substitution ciphers using simulated annealing with fixed temperature." *Proceedings of the 2nd International Conference on Historical Cryptology*, HistoCrypt.

Tomokiyo, S. 2019-2022. *A Polyphonic Substitution Cipher of the Catholic League (1592-1593)*, Cryptiana. Accessed December 22, 2022. http://cryptiana.web.fc2.com/code/mayenne.htm